INTISARI

Dalam era modern ini, keamanan jaringan sangat penting untuk memastikan ketersedian layanan yang berkelanjutan dan perlindungan terhadap ancaman cyber. Kelemahan dalam sistem keamanan menjadikan penyebab utama pencurian data dan serangan cyber. sistem menjaga keamanan tersebut melalui monitoring lalu lintas pada jaringan. Cacti merupakan aplikasi web berbasis open-source yang menggunakan SNMP (Simple Network Management Protocol) dengan menggunakan SNMP informasi yang diperoleh berupa besaran lalu lintas yang terjadi pada sebuah interface yang dimonitoring. Akan tetapi, penting untuk diketahui Cacti memiliki potensi kerentanan keamanan, salah satu kerentanan yang ditemukan dalam aplikasi cacti adalah CVE-2022-46169. Hal tersebut melatarbelakangi penelitian ini, diperlukan solusi yang mempermudahkan dan mempersingkat proses penetration testing untuk kerentanan CVE-2022-46169. penelitian ini bertujuan untuk membangun sebuah program otomatisasi mampu melakukan pemindaian, mendeteksi kerentanan, mengeksploitasi dan melakukan pembuatan laporan secara otomatis kerentanan CVE-2022-46169 pada aplikasi web Cacti berbasis Python dan Shodan dengan harapan dapat mempermudah dan mempersingkat proses pengujian penetration testing. Pengujian pada penelitian ini dibagi menjadi dua bagian, yaitu uji fungsionalitas program otomatisasi dan uji perbandingan waktu antara metode manual dengan metode menggunakan program otomatisasi. hasil dari penelitian ini menunjukan bahwa program mempu melakukan keseluruhan fungsional untuk melakukan pengujian penetration testing, mulai dari proses pemindaian, mendeteksi kerentanan, eksploitasi, pembuatan laporan serta mengunggah hasil laporan kedalam repositori github. Dengan diterapkanya program otomatisasi ini, proses uji penetration testing kerentanan CVE-2022-46169 pada aplikasi web Cacti mengalami penyusutan sebesar 30.08% pada opsi *local,* sedangkan opsi public mengalami penyusutan sebesar 51.36% ketika menggunakan program otomatisasi.

Kata kunci: Otomatisasi, *Penetration Testing*, CVE-2022-46169, Cacti, Python, Shodan, *Metasploit*.

ABSTRACT

In today's modern era, network security is crucial for ensuring the continuous availability of services and protection against cyber threats. Vulnerabilities in security systems are the main cause of data theft and cyber-attacks. One way to maintain security is through network traffic monitoring. Cacti is an open-source web application that uses SNMP (Simple Network Management Protocol) to obtain information on traffic volumes occurring on monitored interfaces. However, it is important to note that Cacti has potential security vulnerabilities. One such vulnerability is CVE-2022-46169. This study aims to provide a solution that simplifies and speeds up the penetration testing process for the CVE-2022-46169 vulnerability. The objective of this research is to develop an automation program capable of scanning, detecting vulnerabilities, exploiting them, and automatically generating reports on CVE-2022-46169 vulnerability in Cacti web applications. The program will be based on Python and Shodan, with the hope of simplifying and accelerating the penetration testing process. The testing in this study is divided into two parts: functional testing of the automation program and a comparative time study between manual methods and the automated program. The results of this study show that the program can perform the entire penetration testing process, from scanning, detecting vulnerabilities, exploiting them, generating reports, and uploading the report results to a GitHub repository. With the implementation of this automation program, the penetration testing process for the CVE-2022-46169 vulnerability in Cacti web applications saw a reduction of 30.08% in the local option, and a reduction of 51.36% in the public option when using the automation program.

Keywords: Automation, *Penetration Testing*, CVE-2022-46169, Cacti, Python, Shodan, *Metasploit.*